WHAT WE CLAIM IS:

1. A system for controlling devices at a location by an outside entity, the system comprising:

(a) at least one device installed at the location;

(b) an internal computer system in communication with the device, wherein the internal computer system is adapted to control the device; and

(c) a firewall in communication with the internal computer system, wherein the firewall is adapted to verify identity information associated with the outside entity,

wherein when a triggering event is detected at the location, one of the internal computer system and the outside entity initiates a communication session between the internal computer system and the outside entity,

wherein the outside entity provides identity information to the firewall, and

wherein the firewall allows the outside entity to control the device through the internal computer system if the firewall recognizes the identity information.

2. The system of claim 1, wherein control of the communication session rests exclusively with the outside entity.

3. The system of claim 1, wherein the outside entity is an emergency response unit.

4. The system of claim 3, wherein the emergency response unit is a public safety answering point.

5. The system of claim 1, wherein the outside entity is a private security firm.

6. The system of claim 1, wherein the identity information is a password.

7. The system of claim 1, wherein the identity information is a digital certificate.

8. The system of claim 7, wherein the digital certificate is issued and authenticated by a certificate authority.

9. The system of claim 1, further comprising a sensing apparatus in communication with the internal computer system, wherein the triggering event is detected by the sensing apparatus.

10. The system of claim 1, wherein the at least one device is an observation device.

11. The system of claim 1, wherein the at least one device is an emergency response device.

12. The system of claim 1, wherein the internal computer system is a local area network.

13. The system of claim 1, wherein the communication session uses transmission control protocol.

14. The system of claim 1, wherein the communication session uses digital communications protocol.

15. A method for controlling devices at a location by an outside entity, the method comprising the steps of:

(a) associating at least one device with an internal computer system at the location;

(b) requesting the outside entity to control the at least one device;

(c) establishing a communication session between the outside entity and the internal computer system;

(d) authenticating the identity of the outside entity; and

(e) allowing the outside entity to control the at least one device through the internal computer system.

16. The method of claim 15, wherein only the outside entity can terminate the communication session.

17. The method of claim 15, wherein the at least one device is an observation device.

18. The method of claim 15, wherein the at least one device is an emergency response device.

19. The method of claim 15, wherein the outside entity is an emergency response unit.

20. The method of claim 15, wherein the outside entity is a private security firm.

21. The method of claim 15, wherein the outside entity is a healthcare provider.

22. The method of claim 15, wherein the internal computer system is a local area network.

23. The method of claim 15, wherein the internal computer system is Bluetooth compatible.

24. The method of claim 23, wherein the at least one device is Bluetooth-enabled.

25. The method of claim 15, further comprising the step of transferring the communication session from the outside entity to a third party.

26. The method of claim 15, wherein the third party is an emergency response unit.

27. The method of claim 15, wherein the communication session uses transmission control protocol.

28. The method of claim 15, wherein the communication session uses digital communication protocol.

29. The method of claim 15, wherein the identity of the outside entity is authenticated by a certificate authority.

30. The method of claim 15, wherein the identity of the outside entity is authenticated by the internal computer system based on a password provided by the outside entity.

31. A system for enabling an outside entity to control devices at a location, the system comprising:

(a) an internal computer system associated with the location;

(b) a sensing apparatus associated with the internal computer system, wherein the sensing apparatus can detect a triggering event at the location;

(c) a firewall in communication with the internal computer system, wherein the firewall is adapted to verify identity information associated with the outside entity; and

(d) a device associated with the internal computer system, wherein the device can be controlled by the outside entity via the internal computer system,

wherein when the sensing apparatus detects the triggering event the internal computer system establishes a communication session with the outside entity via an external computer network,

wherein the outside entity provides identity information to the internal computer system,

wherein the firewall creates a secured tunnel for the outside entity to access the internal computer system,

wherein the outside entity uses information retrieved from a database to control the device during the communication session, and

wherein only the outside entity can terminate the communication session.

32. The system of claim 31, wherein the identity information comprises a password.

33. The system of claim 31, wherein the identity information comprises a digital certificate.

34. The system of claim 33, wherein the digital certificate is authenticated by a certificate authority.

35. The system of claim 31, wherein the external computer network is the Internet.

36. A method for enabling an outside entity to control devices at a location, the method comprising the steps of:

(a) associating at least one device with an internal computer system at the location;

(b) reporting a triggering event associated with the location to the outside entity;

(c) initiating a communication session between the internal computer system and the outside entity through an external computer network, wherein the communication session is initiated by the internal computer network;

(d) verifying identity information provided by the outside entity; and

(e) allowing the outside entity to control the device during the communication session,

wherein only the outside entity can terminate the communication session.

37. The method of claim 36, wherein the identity information is a password issued to the outside entity by the internal computer system.

38. The method of claim 36, wherein the identity information is a digital certificate issued to the outside entity by a certificate authority.

39. The method of claim 38, wherein the step of verifying the identity information of the outside entity is performed by the certificate authority.

40. The method of claim 36, further comprising the step of authenticating identity of the internal computer system for the outside entity.

41. A method for enabling an outside entity to handle a situation at a location, the method comprising the steps of:

(a) associating at least one device with an internal computer system at the location;

(b) reporting a triggering event associated with the situation at the location to the outside entity;

(c) initiating a communication session between the internal computer system and the outside entity through an external computer network;

(d) providing a first identity information associated with the internal computer system to the outside entity;

(e) providing a second identity information associated with the outside entity to the internal computer system;

(f) authenticating both the first identity information and the second identity information;

(g) establishing a secured tunnel through a firewall associated with the internal computer system if both the first identity information and the second identity information are authenticated; and

(h) allowing the outside entity to control the device to handle the situation during the communication session,

wherein only the outside entity can terminate the communication session.

42. The method of claim 41, wherein the first identity information is a first digital certificate issued to the internal computer system by a certificate authority.

43. The method of claim 41, wherein the second identity information is a second digital certificate issued to the outside entity by a certificate authority.

44. The method of claim 41, wherein the step of authenticating both the first identity information and the second identity information is performed by a certificate authority.